

RECEIVED
CENTRAL FAX CENTER

Patent Application SEP 21 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	MESSERGES ET AL.	EXAMINER:	ABYANEH
SERIAL NO.:	10/028,164	GROUP:	2133
FILED:	25 OCT 2001	CASE NO.:	CR00287M
TITLED:	A METHOD FOR EFFICIENT HASHING OF DIGITAL CONTENT		

Motorola, Inc.
Corporate Offices
1303 E. Algonquin Road
Schaumburg, IL 60196
September 20, 2005

Declaration Under 37 CFR §1.131

Each of the undersigned, Thomas Messerges, Ezzat Dabbish, Larry Puhl, and Douglas Kuhlman declare the following:

1. Prior to March 21, 2001, we conceived of the invention in the United States now claimed in US Patent application number 10/028,164.

2. As evidence of the conception date of the pending application, enclosed is a copy of a Motorola Patent Disclosure Form in the form of a true copy of the original. The Motorola Patent Disclosure Form was created by us in the United States and witnessed by a third party prior to March 21, 2001.

In paragraph 5, entitled "What is the invention being disclosed:", the Inventors show conception of the invention, stating that "the first step is to encrypt the content . . . the content is split into smaller "chunks" . . . [and] the cryptographic has of each of these chunks is then calculated and stored into a "hash table" . . . then signed"

3. We exercised due diligence from prior to March 21, 2001 to October 25, 2001 to prepare and file the pending patent application number 10/028,164. During

REST AVAILABLE COPY


this time period, we continually worked toward preparing the pending patent application for filing with the USPTO. As evidence of such diligence, the Applicants are submitting the following documents:

1. Inventor report (page 4) that in February 2001, the invention was submitted to the Motorola Patent Committee;
 2. Inventor report (page 4) that on June 22, 2001 the Motorola Corporate Patent Committee decided to pursue this disclosure;
 3. A copy of an email dated July 24, 2001 to Michelle Larsen asking for quotes to prepare a patent application for the invention;
 4. A copy of a Federal Express shipping receipt showing that materials needed to establish a quote, dated July 24, 2001;
 5. An email dated August 14, 2001 showing acceptance of the quoted price;
 6. Inventor reports for week ending 9-21-2001 showing the inventors plan to review the "hash table patent" from Michelle (Larsen);
 7. Inventor reports for week ending 9-28-01: reports that the inventors reviewed the hash table patent and rewrote the claims;
 8. Inventor reports for week ending 10-12-01: reports that inventors "Completed final review of the Fast Hash patent"
 9. Emails dated 10-23-2001 and 10-25-2001 showing the inventors intent on signing off on the patent filing.
4. All of the above statements made of our own knowledge are true and all statements made on information and belief are believed to be true.

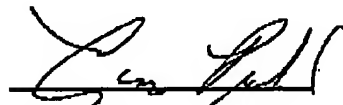
5. We understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 USC §1001) and may jeopardize the validity of the pending application or any patent issuing thereon.


Thomas Messerges

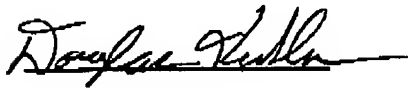
9-20-05
Date


Ezzat Dabbish

9/20/05
Date


Larry Puhl

9/20/05
Date


Douglas Kuhlman

9/20/2005
Date

Motorola Patent Disclosure - Additional Information

Page 1

**MOTOROLA LABS**

Disclosure for Patent Committee Review
Submitted Pursuant to Employee Agreement
DISCLOSURE TYPE:



Disclosure Number CR00287M	Date February 15, 2008
Division(s): Corporate	
Patent Committee Action:	

SHORT FORM

☐

When using the short form (single page), the review committee may request additional information before reaching a decision.

EXPANDED

☒

Use additional pages in the expanded form if you feel more information will be necessary for the committee to reach a decision.

1. Title of Invention: A Method for Securely Binding Usage Rules to Digital Content 1a. Key Words: Digital Rights Management (DRM), Digital Content, Content Protection, Hash, Certificate

2. Primary or contact point inventor(s) (Use your full first, middle and last names. Use page 2 of the expanded disclosure form for contributing inventors).

1)	Thomas S. Messerges Name US Citizenship	328-60-0086 SSN	151 Brookston Drive Street	AE575 Dept. No.	IL02 Rm 2712 Location/Rm. # Schaumburg City	847-576-5827 Phone Number IL 60193 State ZIP
2)	Ezzat A. Dabbish Name US Citizenship	329-50-0221 SSN	445 Adare Drive Street	AE575 Dept. No.	IL02 Rm 2712 Location/Rm. # Cary City	847-576-5377 Phone Number IL 60013 State ZIP
3)	Larry Puhl Name US Citizenship	328-38-5125 SSN	1231 Fawn Hallow Street	AE579 Dept. No.	IL02 Rm 2256 Location/Rm. # West Dundee City	847-576-5453 Phone Number IL 60118 State ZIP
4)	Douglas A. Kuhlman Name US Citizenship	510-88-0815 SSN	1447 Ashwood Ct Street	AE575 Dept. No.	IL02 Rm 2712 Location/Rm. # Elgin City	847-576-9675 Phone Number IL 60123 State ZIP

3. What was the problem(s) to be solved by the invention or what was the need(s) for the invention:

The popularity of digital content, such as MP3 music files, electronic games, and DVD movies, is growing at a tremendous rate. Portable, wireless devices are on the verge of making access to this digital content easier than ever. Content owners, however, are worried, that with the advent of these new devices, their digital content will become more susceptible to illicit copying and distribution. In order to avoid widespread piracy, like that prevalent on the Internet (e.g., Napster), there is a need for secure methods to distribute electronic content that are not subject to abuse.

Digital Rights Management (DRM) is a popular phrase used to describe the protection of rights and the management of rules related to accessing and processing digital information. These rights and rules govern various aspects of a digital object, such as who owns the object, how and when an object can be accessed, and how much an object may cost. Content owners hope to use a secure, tamper-resistant DRM system to enforce the rules associated with a digital object. If the rules say that a digital song cannot be copied, then the DRM system will not copy it. Likewise, if the rules say that playing a DVD movie will cost \$3, then the DRM system will debit the consumer's credit card by \$3. Hackers should not be able to overcome the enforcement of these rules or alter the content associated with these rules. In particular, hackers should not be able to alter digital objects or their rules without detection.

The problem of protecting digital objects and their rules is not straightforward. Hackers will likely have direct access to the digital objects and the rules. For example, objects and rules may be stored on the disk drive of a PC where they can be readily accessed by an editing program. Therefore, since hackers will be able to easily change bits in the digital objects or the rules, the DRM system will need to detect such changes.

The size of the digital object can become very large. For example, compressed digital songs are typically 3 to 5 Mbits and DVD movies can be orders of magnitude larger. Verifying that such a large digital object has not been altered can be very time consuming. Our invention solves this problem by providing an efficient method to detect changes in digital objects and their associated usage rules.

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED

4. What is the prior art, and why doesn't it resolve the problem(s) or fulfill the need(s):

In our situation, the content and usage rules constitute a digital object that we refer to as a "content package". A well-known prior-art method for authenticating the integrity of a digital object uses a digital signature scheme to sign a cryptographic hash of the object. A prior art solution using a digital signature scheme and hash to protect digital content is depicted in Figure 1. According to Figure 1, the first step is to encrypt the content. The content is encrypted with a secret key to protect it from being used by anyone other than content purchaser. The encrypted content is then cryptographically hashed to produce Hash(EC). This hash value is placed into the certificate CCert. The CCert certificate also contains the content's usage rules along with the content decryption key that is assigned to the content purchaser using public-key cryptography. Finally, a trusted authority digitally signs the certificate.

Verifying the authenticity of a content package is simple. The first step is to verify the signature of the digital signature of CCert. Once this signature is verified, the hash of the encrypted content is recalculated and compared to the value in the certificate. If digital signature is valid and the hash values match, then the content package is deemed authentic. The rendering of content can begin only after the content package has been authenticated.

The main problem with this prior-art solution is that it can take too long to calculate the hash of the entire content package. A user of a content rendering device expects rendering to begin immediately. After pressing the play button of an MP3 player, the song should start playing with minimal delay. If the prior-art method is used, then the hash of the entire content needs to be calculated before the usage rules can be verified. This could be very time consuming. For example, the estimated time to compute the SHA1 hash of a typical MP3 song, when using a 16 MHz MCore processor, is around 15 to 20 seconds. Clearly this is too long and a more efficient method is needed. More background on prior-art data authentication solutions can be found in standard cryptography textbooks such as:

Douglas R. Stinson, "Cryptography: Theory and Practice," CRC Press, 1995.

5. What is the invention being disclosed:

Our invention eliminates the need to calculate the hash of the entire content package before rendering the content. Instead, the hash is calculated incrementally and verified as the content is being rendered.

Our invention is depicted in Figure 2. As in the prior-art solution the first step is to encrypt the content. Next, however, the content is split into smaller "chunks". The cryptographic hash of each of these chunks is then calculated and stored into a "hash table". The entries of the hash table are then hashed to create an "overall hash". The overall hash is placed into the certificate CCert that is then signed by a trusted authority.

The advantages of our scheme become apparent when authenticating the content package. Figure 3 shows that our authentication procedure begins with a verification of the hash table. The overall hash of the hash table is recalculated and then compared to the hash value in the CCert certificate. If the hash values agree and the signature on CCert is valid, then the hash table and its binding to the usage rules is verified. Since the overall hash is not over the entire content, but just the hash table, it can be quickly calculated.

Once the overall hash has been authenticated, the hash of the individual chunks can be verified. Figure 4 shows our procedure for verifying the authenticity of a chunk. The first step is to recalculate the hash table entry of the chunk and compare it to the actual hash value in the hash table. Since the hash table has already been authenticated, agreement of the hash values implies that the chunk is authentic. It should be noted that the computation of a chunk's hash is not as time consuming as computing the hash of the entire content package. Also, this hash value can be calculated in parallel to the chunk decryption. Thus, rendering can begin almost immediately.

6. How does this invention resolve the problem(s) and fulfill the need(s) in a new way:

(Attach any drawings or diagrams you feel are necessary for clarification)

The problem of authenticating digital content and its binding to usage rules was solved using a divide-and-conquer approach. Our invention calls for the authentication to be conducted in two phases. The first phase provides assurance that the hash table is authentic and bound to the certificate and rules. This phase can be calculated very quickly since only the hash of the hash table needs to be computed. By hashing the hash table, hackers are prevented from deleting, adding, or rearranging the content chunks.

The second phase of our invention verifies the authenticity of every content bit. The hash of the content chunk is compared to the hash table entry to provide final assurance that the content is bound to the certificate and rules. This hash can be calculated one chunk at a time, parallel to decryption, to enable immediate rendering.

Our invention is even applicable to protecting extremely large content files (i.e., video). In this situation, the hash table can be very large and even calculating the overall hash becomes too slow. Our invention, with a minor modification, can handle this problem by allowing the hash table to be subdivided into chunks that are subsequently hashed and added to a secondary hash table. The resulting scheme then uses multiple layers of hash tables and a single certificate to authenticate all of the hash tables and the content.

Overall, the disclosed invention provides an efficient means to authenticate digital content and bind the content to usage rules. The security of our scheme is equivalent to prior art methods, while the efficiency is improved.

7. Date of conception: January, 2001 and if applicable, date first built (or written) and successfully tested:

8. Product(s) this invention may be used in:

Future Motorola pagers, mobile phones, automotive entertainment systems, and set-top boxes that handle digital content such as music books, and video.

9. Date the first offer for sale was made for a product incorporating this invention:

None, but there are plans to discuss our secure content distribution system with Vivendi/Universal and Disney.

10. Date the first disclosure of this invention was made outside Motorola without a nondisclosure agreement:

None, but disclosure during an SDMI meeting is being considered.

11. Approvals: 1) Technical Staff or Patent Liaison 2) Management (both required) - Signing this form attests to the fact that you understand the invention.

	Name/Signature	Dept. No.	Location/Rm. #	Phone Number
	<i>[Signature]</i> Larry Puhli	AE579	IL02	6-5463
2)	STEVE LEINE <i>[Signature]</i>	AE570	IL02	6-2107

12. Witnesses:

Witness: *[Signature]*

Date: 2/19/01 Witness: *[Signature]*

Date: 2/19/01

13. Contributing Inventor(s): Patent Department will determine legal inventorship

	Name	Signature	Dept. No.	Location/Rm. #	Phone Number
	Citizenship	SSN	Street	City	State ZIP
5)					
6)					
7)					
8)					

14. What is the business impact of having a patent on this invention, for Motorola and/or competition:

It is in Motorola's interest to ensure that their products uphold the emerging security requirements for managing digital data, while also providing for an enjoyable user experience for our consumers. Our disclosed invention provides a novel method to improve a user's experience by ensuring that their content can be rendered without delays or interruptions due to annoying DRM requirements.

Being first to market with a Digital Rights Management system that does not hinder the end user will secure Motorola's leadership in the industry. Other organizations may mandate the use of our solution, in which case financial gains can be made from licensing and royalty fees. In addition orders for our products can be expected to increase as a result of our name being tied to a secure and user friendly solution.

15. Expanded description; list any additional details you feel would be helpful in describing the invention:

16. Additional details concerning the prior art related to this invention:

Attach any backup documents or provide any other information you feel would be helpful in determining the desirability of obtaining a patent on this invention. Any attachments that are critical to the disclosure of the invention should be witnessed.

See attached Figures 1 to 4.

Additional Information:

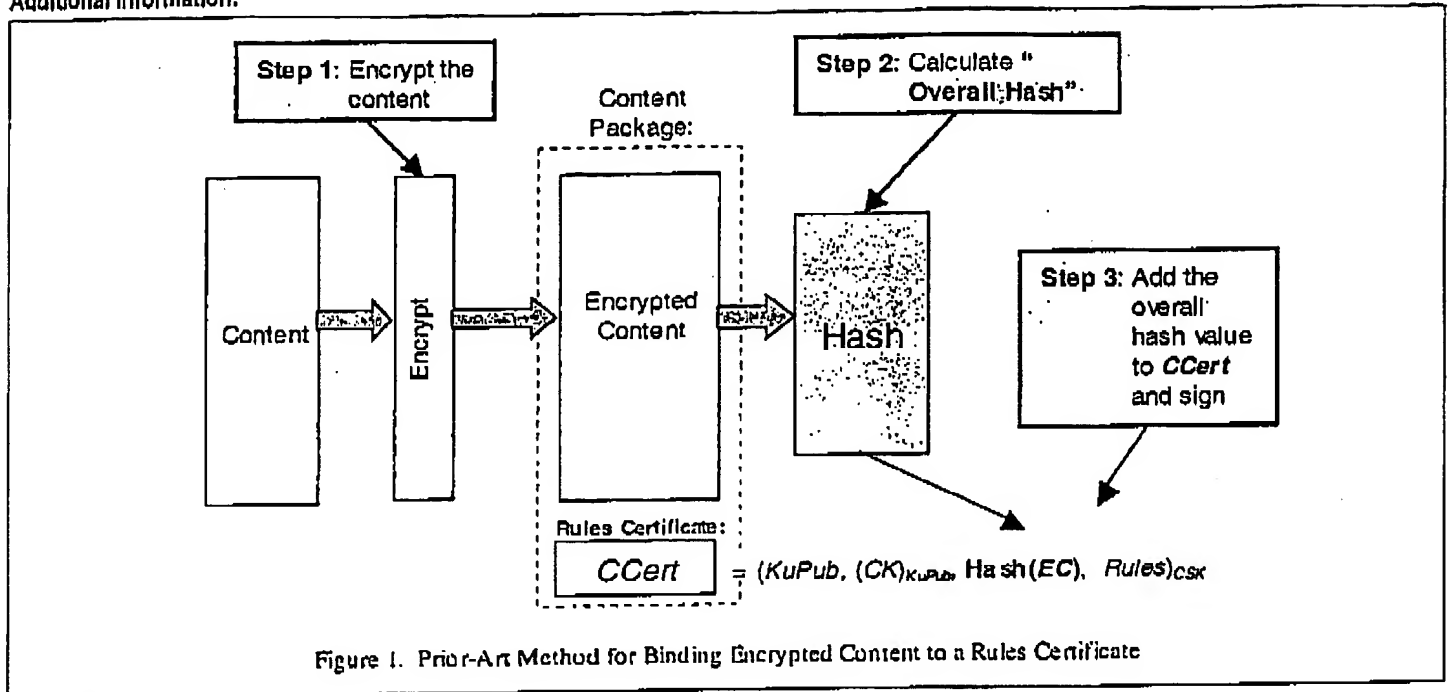


Figure 1. Prior-Art Method for Binding Encrypted Content to a Rules Certificate

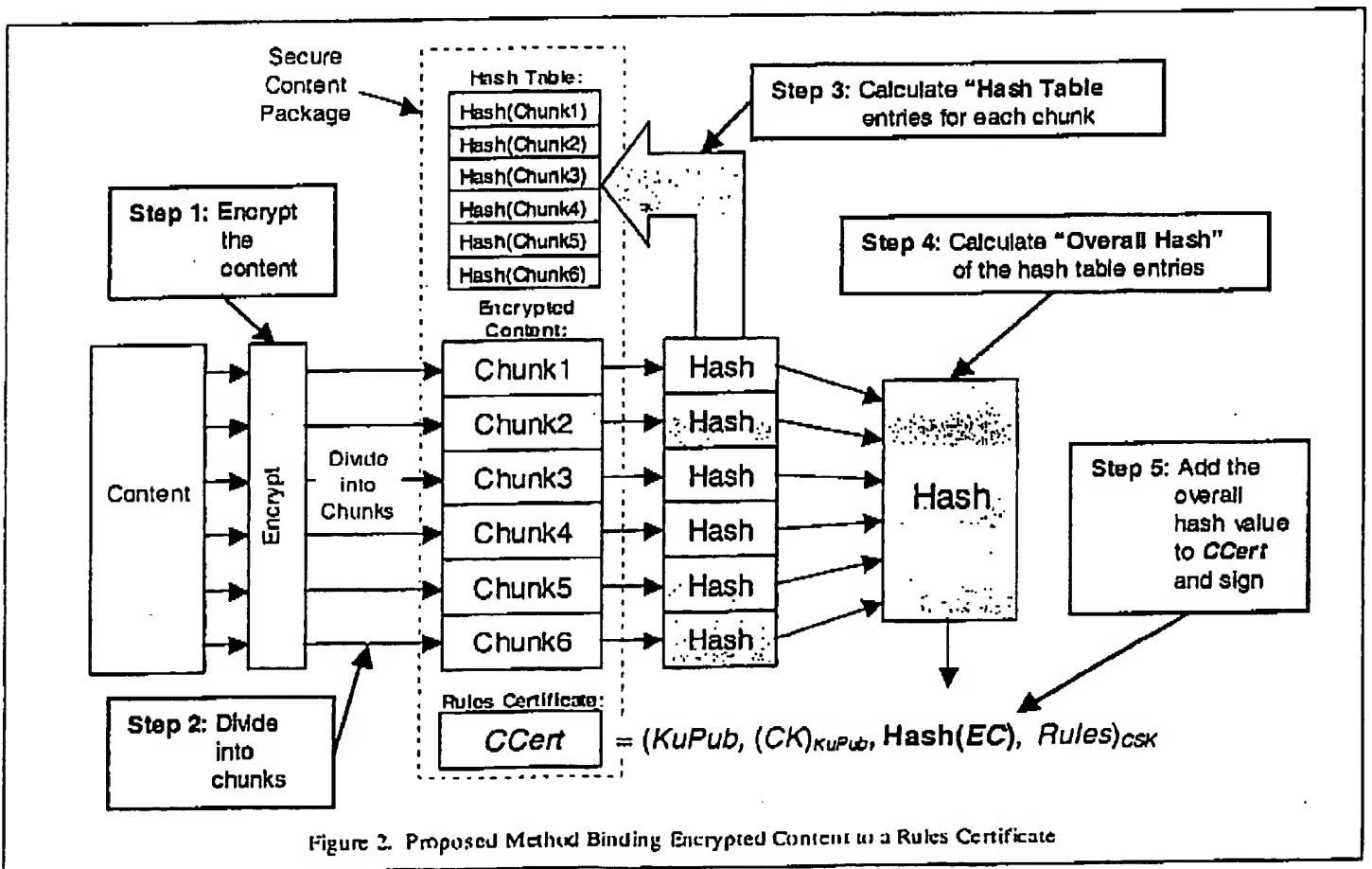


Figure 2. Proposed Method Binding Encrypted Content to a Rules Certificate

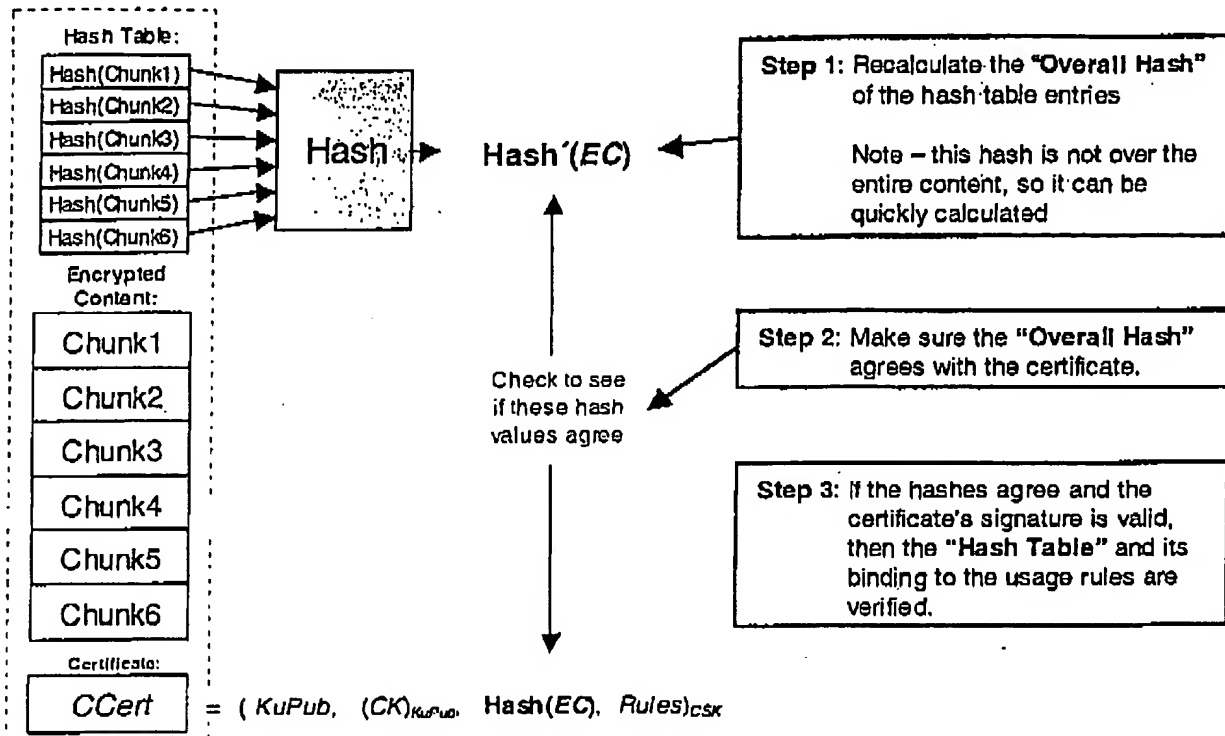


Figure 3. Proposed Method for Verifying a Content Package's "Hash Table"

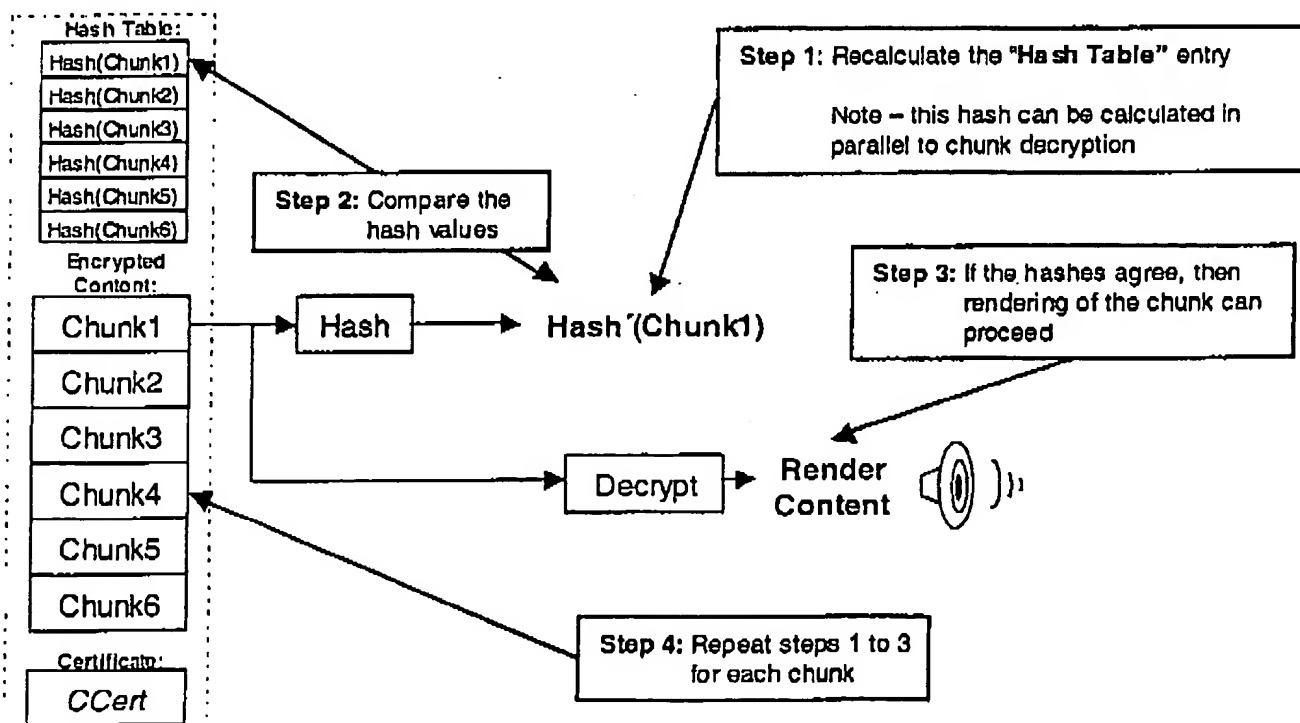


Figure 4. Proposed Method for Verifying a Content Package's Content "Chunks"



Motorola Confidential Proprietary

2000-575-01

Page 4

February 2001

and Larry Puhl, was submitted to the Motorola Corporate Patent Committee. This patent describes a DRM system using domains rather than check-in and check-out.

A patent disclosure (CR00287M) dated February 15th, 2001 and titled "A Method for Securely Binding Usage Rules to Digital Content," by Tom Messerges, Ezzy Dabbish, Larry Puhl, and Doug Kuhlman, was submitted to the Motorola Corporate Patent Committee. This patent describes an efficient cryptographic hashing scheme for binding DRM rules to digital content.

A patent disclosure (CR00288M) dated February 15th, 2001 and titled "A Method and System for Block Cipher Encryption Using a Large S-box, Potentially Keyed by a Stream Cipher," by Doug Kuhlman, was submitted to the Motorola Corporate Patent Committee. This patent describes DECK, a content encryption algorithm.

A patent disclosure (CR00289M) dated February 21th, 2001 and titled "A Method for Preventing Information Leakage During a Squaring Operation," by Tom Messerges and Doug Kuhlman, was submitted to the Motorola Corporate Patent Committee. This patent describes an efficient method to randomize the squaring operation used in the DECK algorithm.

Future Plans

1. Distribute the DECK white paper for further review and cryptanalysis.
2. Develop a DRM demonstration system to show how a music can be securely distributed from a kiosk to Motorola products via Bluetooth.
3. Continue writing a white paper titled "A Framework for Managing Digital Content in Motorola Products".
4. Develop a presentation to describe management of digital content in Motorola's wireless products.
5. Keep abreast of the security aspects of the SDMI activities.
6. Keep abreast of watermarking technologies and how these technologies will impact Motorola's products.

Responsible Engineers:

Ezzy Dabbish
Brian King
Doug Kuhlman
Yi Li
Tom Messerges
Dean Vogler



Motorola Confidential Proprietary



Motorola Confidential Proprietary

2000-575-01

Page 4

June 2001

Patent Status

A patent disclosure (CR00286M) dated February 12th, 2001 and titled "System and Method for Secure and Convenient Management of Electronic Content," by Tom Messerges, Ezzy Dabbish, and Larry Puhl, was submitted to the Motorola Corporate Patent Committee. This patent describes a DRM system using domains rather than check-in and check-out. The concepts of this patent were filed in a provisional application on April 18, 2001. On June 22, 2001, the Motorola Corporate Patent Committee decided to pursue this disclosure.

A patent disclosure (CR00287M) dated February 15th, 2001 and titled "A Method for Securely Binding Usage Rules to Digital Content," by Tom Messerges, Ezzy Dabbish, Larry Puhl, and Doug Kuhlman, was submitted to the Motorola Corporate Patent Committee. This patent describes an efficient cryptographic hashing scheme for binding DRM rules to digital content. On June 22, 2001, the Motorola Corporate Patent Committee decided to pursue this disclosure.

A patent disclosure (CR00288M) dated February 15th, 2001 and titled "A Method and System for Block Cipher Encryption Using a Large S-box, Potentially Keyed by a Stream Cipher," by Doug Kuhlman, was submitted to the Motorola Corporate Patent Committee. This patent describes DECK, a content encryption algorithm. On June 22, 2001, the Motorola Corporate Patent Committee decided to pursue this disclosure.

A patent disclosure (CR00289M) dated February 21th, 2001 and titled "A Method for Preventing Information Leakage During a Squaring Operation," by Tom Messerges and Doug Kuhlman, was submitted to the Motorola Corporate Patent Committee. This patent describes an efficient method to randomize the squaring operation used in the DECK algorithm. On June 22, 2001, the Motorola Corporate Patent Committee decided not to pursue this disclosure, but instead to send it to Motorola BCS for their consideration.

Future Plans

1. Continue the cryptanalysis and development of DECK software.
2. Develop a DRM demonstration system to show how a music can be securely distributed from a kiosk to Motorola products via Bluetooth.
3. Continue to consult with product groups and develop presentations describing content management strategies for future Motorola products.
4. Keep abreast of the security aspects of the SDMI activities.
5. Keep abreast of watermarking technologies and how these technologies will impact Motorola's products.

Responsible Engineers:

Ezzy Dabbish
Brian King
Doug Kuhlman

Yi Li
Tom Messerges
Dean Vogler



Motorola Confidential Proprietary

(3)

Donlin Leo-ALD080

From: Juffernbruch Dan-ADJ001
Sent: Tuesday, July 24, 2001 3:14 PM
To: Michelle Larson (E-mail)
Cc: Donlin Leo-ALD080; Nichols Dan-ECOR01
Subject: FW: FedEx shipment 791618890230

Michelle,

We have sent you a Fed Ex package today and would like quotes on two additional patent applications for disclosures CR00286M and CR00287M. One was already filed as a provisional application and we have also sent a copy of the provisional filing.

The two are in the area of Digital Rights Management DRM. I can explain the portfolio area sometime when we speak in the future.

Thanks,
Dan

Dan Juffernbruch
Division Patent Counsel
Motorola Law Department
Corporate Offices
1303 E. Algonquin Rd, Schaumburg, IL 60196
847-538-3129; 775-806-3679 fax
Dan.Juffernbruch@motorola.com

"Visionary companies like Motorola don't see it as a choice between living to their values or being pragmatic; they see it as a challenge to find pragmatic solutions and behave consistent with their core values." Built to Last, Collins & Porras (c)1994.

This electronic transmission (and any attached document) is for the sole use of the individual or entity to whom it is addressed. It is confidential and may be subject to attorney/client privilege. Any further distribution or copying of this message is strictly prohibited. If you received this message in error, please notify me, and destroy the attached message (and all attached documents), immediately.

-----Original Message-----

From: Karen Kass-AKK019 [mailto:Karen_Kass-AKK019@email.mot.com]
Sent: Tuesday, July 24, 2001 2:17 PM
To: Dan.Juffernbruch
Subject: FedEx shipment 791618890230

KAREN KASS of MOTOROLA, INC sent MICHELLE LARSON of LARSON & ASSOCIATES a Standard Overnight FedEx Envelope.

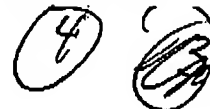
This shipment is scheduled to be sent on 24JUL01.

The sender included the following message:

"Dan Juffernbruch is sending copies today, via FedEx, of two disclosures: CR00286M and CR00287M. He would like you to
1"

The tracking number is 791618890230.

To track this shipment online click on the following link:
http://www.fedex.com/cgi-bin/tracking?tracknumbers=791618890230&action=track&language=english&cntry_code=us



July 24, 2001

VIA FEDERAL EXPRESS

Michelle Larson
Larson & Associates
221 East Church Street
Frederick, MD 21701

Dear Ms. Larson:

Attached please find copies of two disclosures: CR00286M and CR00287M. Daniel Juffernbruch would like you to look at these and submit an estimate for the costs of producing specifications for both cases.

CR00286M was filed provisionally April 18, 2001. The documents filed with the case are attached.

The inventors are all in Schaumburg and are the same on both cases with the exception of one additional inventor on CR00287M.

If you have any additional questions, please contact Dan at 847-538-3129.

Very truly yours,
MOTOROLA, INC.

Karen Kass, Assistant to
Daniel W. Juffernbruch
Patent Attorney

DWJ: kgk

✓ C: Leo Donlin

Corporate Offices
1303 E. Algonquin Road, Schaumburg, IL 60196 (847) 538-3129
Fax No. (847) 576-3750

From: KAREN KASB (847)576-6364
MOTOROLA, INC
1303 E. ALDONQUIN ROAD
IL01, 3RD FLR
SCHAUMBURG, IL, 60186

SHIPPER'S FEDEX ACCOUNT #



FedEx.

To: MICHELLE LARSON (301)668-3073
LARSON & ASSOCIATES
221 East Church Street

SHIP DATE: 24JUL01
WEIGHT: 1 LBS

FREDERICK, MD, 21701

Ref: AC934 DISCLOSURES



DELIVERY ADDRESS BARCODE FEDEX-EPN

TRK # 7916 1889 0230 6201

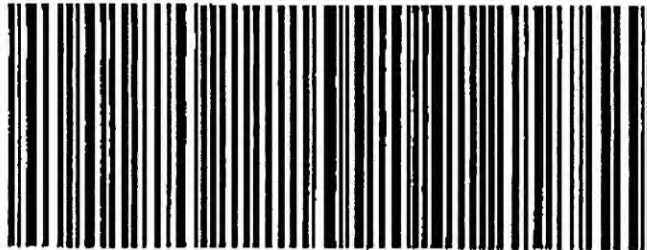
FedEx STANDARD OVERNIGHT

21701-MD-US

NH FDKA

WED
AA

Deliver by:
25JUL01



Please fold this document in half and place it in the waybill pouch affixed to your shipment so that the barcode portion of the label can be read and scanned.
***WARNING: Use only the printed original label for shipping. Using a photocopy of this label for shipping purposes is fraudulent and could result in additional billing charges, along with the cancellation of your FedEx account number.

Shipping Label

[Schedule Courier](#)

[Find a Drop-off Location](#)

[Shipping History](#)

[Shipment Complete](#)

[Cancel Shipment](#)

1. Use the "Print" feature from your browser to send this page to your laser or inkjet printer.
2. Fold the printed page along the horizontal line.
3. Place label in shipping label pouch and affix it to your shipment so that the barcode portion of the label can be read and scanned.
4. To print a receipt of your shipment, please click on "Shipping History."

Ship a New Package

[Ship Inside U.S.](#)

[Ship Outside U.S.](#)

[Ship to Same Recipient](#)

Use of this system constitutes your agreement to the service conditions in the current FedEx service Guide, available upon request.

FedEx will not be responsible for any claim in excess of \$100 per package, whether the result of loss, damage, delay, non-delivery, misdelivery, or misinformation, unless you declare a higher value, pay an additional charge, document your actual loss and file a timely claim. Limitations found in the current FedEx Service Guide apply. Your right to recover from FedEx for any loss, including intrinsic value of the package, loss of sales, income interest, profit, attorney's fees, costs, and other forms of damage whether direct, incidental, consequential, or special is limited to the greater of \$100 or the authorized declared value. Recovery cannot exceed actual documented loss. Maximum for items of extraordinary value is \$500, e.g. jewelry, precious metals, negotiable instruments.

Donlin Leo-ALD080

From: Jufferbruch Dan-ADJ001
Sent: Tuesday, August 14, 2001 4:01 PM
To: 'Michelle Larson'
Cc: Nichols Dan-ECOR01; Donlin Leo-ALD080
Subject: RE: Quotes

Michelle,

These quotes look good. See you in the morning.

Dan

-----Original Message-----

From: Michelle Larson [mailto:michelle@larsonpc.com]
Sent: Tuesday, August 14, 2001 1:24 PM
To: Jufferbruch Dan-ADJ001
Cc: Nicholas Dan-ECOR01; Michelle Larson
Subject: Quotes

The following quotes include planned travel to visit the inventors. If not needed, the invoice will be lowered accordingly.

MR00286M	\$7,300
MR00287M	\$6,800
MR00245M	\$6,700
ML00031D	\$5,950
ML00036H	\$6,450
ML00032D	\$5,700
ML00059-D	\$7,450

Look forward to meeting you tomorrow.

Best regards,
Michelle Larson
Larson & Associates, P.C.
21 East Church Street
Frederick, MD 21701
410-668-3073

(6)

From To:dabbish Mon Sep 24 09:24:23 2001
Date: Mon, 24 Sep 2001 9:24:23 CDT
To: dabbish@labs.mot.com (Bzzy Dabbish)
Subject: Week Ending 9-21-01
Cc: yli@labs.mot.com (Yi Q. Li)

~~Week: Ending 9-21-01~~

- Completed three RMTR posters:
TRUST, SDR, Domain diagram
The final copy of all RMTR posters and handouts is on
deltona: shared/drm/rmtr_2001
- Participated in RMTR tech fair.

Short Term Plan:

- Meet with Terri Hughes regarding EPC scrambling patent
- ~~Review hash table patent from Michelle~~
- Work with John Kroupa of GTSS to define and implement security for
upgradable base station project.
- Work with Alan Bok to get him started on integrating our security
software with his Java system.
- Review DRM specification for upcoming Nokia meeting.
- Work with Yi to define future DRM demonstration system goals.
- Revise the streaming section in our white paper.

7

From To:dabbish Mon Oct 1 09:24:16 2001
 Date: Mon, 01 Oct 2001 9:24:16 CDT
 To: dabbish@labs.mot.com (Ezzy Dabbish)
 Subject: Week Ending 9-28-01
 Cc: yli@labs.mot.com (Yi Q. Li)

~~Week Ending 9-28-01~~

- Worked with Terri Hughes to complete EPC scrambler patent. Doug and I reviewed the spec and worked on the claims. Terri is finalizing things and should have a new version for us to review this week.
- Reviewed hash table patent with Doug and Ezzy. The claims were rewritten and submitted to Michelle for review.
- Met with John Kroupa and Henry Pierce of GTSS to discuss their upgradable base station security needs. We agreed to help them with two functions: a signature and verification functions. They need a solution by December, but would prefer something by mid-November (ideally).
- Worked with Alan Bok to better define his security needs for the SDR project. Contrary to his initial assumptions, he just found out that he does not have any security for establishing a secure-authenticated channel. He will need to rely on us for all the security needs, so the scope of our involvement may increase. In light of these events, we're in the process of reevaluating his overall security needs and also how DRM may fit into an overall security architecture.
- Worked with Yi to define the scope and schedule for completing enhancements to our demo. Dave Kennerley is anxious to show the demo to various audiences in the coming weeks.

Short Term Plan:

- Review DRM specification for upcoming Nokia meeting.
- Continue conversations with GTSS to solidify goals and expected deliverables for the base station project.
- Continue work with Alan Bok to define the security architecture of his SDR demonstration system.
- As needed, work with Yi to complete and test DRM demo enhancements.
- As needed, work with Terri Hughes regarding EPC scrambling patent.
- As needed, review hash table patent from Michelle.
- Revise the streaming section in our white paper.

8

From To:dabbish Mon Oct 15 09:13:29 2001
 Date: Mon, 15 Oct 2001 9:13:29 CDT
 To: dabbish@labs.mot.com (Ezzy Dabbish)
 Subject: Week Ending 10-12-01
 Cc: yli@labs.mot.com (Yi Q. Li)

Week Ending 10-12-01

- Scrambler patent patent was completed and signed
- Completed final review of the Fast Hash patent
- Delivered DRM demo to Dave Kennerley of PCS
- Completed personal commitments
- Completed rewrite of SDR security requirements document

Short Term Plan:

- Send PCS CD-ROM with the DRM demo system.
- Deliver working DRM example to SDR project (including small toolkit build)
- Begin work on NSS project - get crypto code from Doug.
- As needed, review documents: 3GPP requirements, Nokia's ERT questions, DA requirements...

7

Kass Karen-akk019

From: Tom Messerges [Tom_Messerges-ADTL01@email.mot.com]
Sent: Tuesday, October 23, 2001 6:56 AM
To: Kass Karen-akk019
Cc: DABBISH EZZY-AMTE09; PUHL LARRY-ATEC16; KUHLMAN DOUG-ADK031; Juffernbruch Dan-ADJ001
Subject: Re: CR00287M

Karen,

I'm not aware of any prior art. Also, I'll be able to sign the application today or tomorrow - although I have a 2-4pm meeting this afternoon.

Regards,
-Tom Messerges

Kass Karen-akk019 wrote:

>
> Gentlemen, is there any prior art for this case? If so, I will need copies ASAP.
>
> Karen G. Kass
> MOTOROLA, INC.
> Law Department
> 1303 E. Algonquin Road
> Schaumburg IL 60196
> Phone: 847-576-6364
> Fax: 847-576-3750

7

Kass Karen-akk019

From: Ezzy Dabbish [Ezzy_Dabbish-AMTE09@email.mot.com]
Sent: Thursday, October 26, 2001 9:33 AM
To: Kass Karen-akk019
Cc: MESSERGES TOM-ADTL01; DABBISH EZZY-AMTE09; PUHL LARRY-ATEC16; KUHLMAN DOUG-ADK031; Juffembruch Dan-ADJ001
Subject: Re: cr00287m-sh9.tif;cr00287m-sh2.tif;cr00287m-sh3.tif;cr00287m-sh4.tif;cr00287m-sh

Q—

dabbish.vcf

Karen,

I'm not aware of any prior art at the moment. We should be ready to sign the Assignment and Declaration today. Tom just informed me that she is setting up an 11:00 am with you today.

thanks for your help.

-- Ezzy

Kass Karen-akk019 wrote:

> Gentlemen, I have been informed that these are the final checkprints; and the specification is also attached. I have the formals on my desk ready to file. If there are no further changes, please advise of your schedule for signing the Assignment and Declaration. We would like to file this case today. In addition, Doug and Tom have come up with no prior art. Ezzy and Larry, do you know of any prior art? If we don't file the case today or tomorrow, I won't be back in the office until Wednesday of next week.

> Karen G. Kass
 > MOTOROLA, INC.
 > Law Department
 > 1303 E. Algonquin Road
 > Schaumburg IL 60196
 > Phone: 847-576-6364
 > Fax: 847-576-3750

```
-----
> Name: cr00287m-sh9.tif
> cr00287m-sh9.tif Type: TIFF Image (image/tiff)
> Encoding: base64
>
> Name: cr00287m-sh2.tif
> cr00287m-sh2.tif Type: TIFF Image (image/tiff)
> Encoding: base64
>
> Name: cr00287m-sh3.tif
> cr00287m-sh3.tif Type: TIFF Image (image/tiff)
> Encoding: base64
>
> Name: cr00287m-sh4.tif
> cr00287m-sh4.tif Type: TIFF Image (image/tiff)
> Encoding: base64
>
> Name: cr00287m-sh5.tif
> cr00287m-sh5.tif Type: TIFF Image (image/tiff)
> Encoding: base64
>
> Name: cr00287m-sh6.tif
> cr00287m-sh6.tif Type: TIFF Image (image/tiff)
> Encoding: base64
```

CV

Kass Karen-akk019

From: Doug Kuhlman [Doug_Kuhlman-ADK031@email.mot.com]
Sent: Tuesday, October 23, 2001 9:23 AM
To: Kass Karen-akk019
Subject: Re: CR00287M

Karen,

No prior art that we're aware of. I am available to sign pretty much any time this week -- preferably tomorrow or today. I have a prior commitment today from about 11:15 to 1:30 and that's the only thing on my schedule.

I also have a concern about the drawings. I notice that you still have some old check prints from Earl Yingling. We had asked for some changes which do not appear on these check prints. We will need to make sure they are updated and correct when we do the final signing.

Doug

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.